AUDIT PLAN
ACCEPTABLE USE POLICIES OF OW! ACCOUNTING SERVICES

Objectives

At OAS, we commit to maintain a high level of trust and integrity towards our clients, partners and employees. Protecting company's assets, including those of our clients', partners' and employees in both tangible and intangible forms, is our priority. The Acceptable Use Policy, which is to provide direction on appropriate Use of OAS' IT assets, is developed based on this principle.

We further understand that having a policy in place is only the first step to fulfill this task. Auditing the policy is the next step to ensure that employees are complying with the established policy. Internal Audit will validate and test controls around this policy. Two objectives that we seek in this audit are:

- To ensure that Acceptable Use Policies exist and provide adequate requirement for the security of the environment; and
- To ensure compliance evidence that proper controls exist and are well designed and implemented to safeguard the environment.

Audit Scope

The audit will encompass the examination on Acceptable Use policy and the control environment. Areas the audit is covering are:

1) **Asset Ownership**
   a) Asset Owners will be identified for all OAS IT assets.
   b) Asset Owners will authorize access to the assets under their control.
   c) Asset Owners are to review and confirm appropriate user access annually.
2) **Acceptable Use of IT Assets**
   a) IT assets will only be used for authorized business purposes.
   b) Users must not make unauthorized copies of copyrighted or OAS owned software.
   c) Connecting non-standard mobile devices and/or personal computers to the OAS network is prohibited.
   d) USB ports on all IT assets must be disabled for the use of portable storage media.
3) **Securing and Storing Information**
   a) OAS computer systems used to store or present company information to users or third parties must be secured to OAS IT standards.
   b) Critical business data must always be managed in such a way that at least one copy is always stored on an OAS server.
4) **Labeling and Handling Information**
   a) Computer hard drives and other media containing proprietary information, and/or licensed software must be secured.
   b) Proprietary information and technical data will not be posted on any computer system accessible to the general public or accessible on the general OAS intranet unless protected by further restrictions.
5) **Passwords**
   a) All System/User level passwords creation must comply with the OAS password policy by following passwords length complexity, aging and lockout.
   b) All computing devices are secured with the password-protected screensaver with the automatic activation feature set to 10 minutes or less. All users must lock the screen or log off when the device is unattended.
   c) Password must be protected and login credential should not be revealed to others.
   d) Users must not use another individual's account, or attempt to capture or guess other user's password.
6) **Remote Connectivity**
   a) Remote connectivity will be granted based on business need.
   b) The users are responsible for keeping the device secure and if the device is lost or stolen, the user is responsible to contact the service desk immediately.
7) **Client Security**
   a) Security controls (physical locks, removing or installing of security applications) on desktops and/or laptops assigned to them by the company.
8) **Social Media**
   a) Social media will only be used for authorized business purposes with the approval of the marketing director or authorized manager.
   b) Social media content must be appropriate, accurate and respectful to OAS (including compliance with financial disclosure laws and OAS confidential information).

The audit will not cover the examination of policies other than the Acceptance Use Policy, i.e. Social Security Number Policy, Security Response Policy, Remote Access Policy, Web Application Security Policy, and Work Station Encryption Policy.

Audit Process

Audit Team

Name	Roles	Responsibilities
Christie Vazquez	Director	Planning and Reviewing
Janet Mai	Manager	Planning and Reviewing
Shahla Raei	Senior Associate	Reviewing and Testing
Yee Ann Chen	Associate	Testing
Mai Ta	Associate	Testing

Time & Budget:

The audit will assess and test the effectiveness of the policy and control environment related to the policy in the year of 2015. The audit is budgeted for $675,000 within a timeframe of 30 business days.

Type of Audit

This is an IT audit of Acceptable Use Policy. We will examine all aspects of the Policy that related to IT control environment, including Asset Ownership, Acceptable use of IT assets, Securing and Storing information, Labeling and Handling Information, Password, Remote Connectivity, Client Security and Social Media.

Control Matrix

	Control Objectives	Control Activities	Audit Procedures	Evidence
1. Asset Ownership To ensure data has a defined and accountable owner.	Owners will be identified for all IT assets. These owners will identify the IT assets under their control and ensure that the protection provided corresponds to the business value of the asset.	All assets in the organization are stored in a central configuration management databases with an owner who is an active employee.	- Sample 10% of the assets in the central database, review for ownership and compare owner against a list of active employees. - Review current exceptions on file and confirm that they have appropriate supporting documentation.	- Current export of CMDB to validate ownership - Current list of active employees to compare with ownership in the CMDB - Current exceptions report
	Owners will authorize access to the assets under their control.	There is a logical access process, includes request form, access needed and management signoff to ensure access to company data is reviewed and assigned by the data owner.	- Review 10% sample of the requests to ensure management signed off and the owner provided the access - Review current exceptions on file and confirm that they have appropriate supporting documentation	- Current Logical access procedure - Export of access requests from ticketing system for the audit period - Current exceptions report
	Owners are to review and confirm appropriate user access annually for assets containing proprietary information	On a yearly basis the owners of the assets review and determine appropriate user privileges are in place. The report is signed off by the owner's manager.	- Review the annual reports for management signoff - Review current exceptions on file and confirm that they have appropriate supporting documentation	- Quarterly access verification reports from the audit period - Current exceptions report
2. IT Asset Controls Set of rules that are	IT assets will only be used for authorized business purposes.	HR monitors computer activity weekly using compliance software	- Review 20% of the compliance reports	- Compliance reports for audit period

designed to protect the organizational resources by establishing a policy and procedure for asset control. These policies will help prevent the loss of data or organizational assets and will reduce risk of losing data due to poor planning.	Users must not make unauthorized copies of copyrighted of OAS owned software.	Inventory of computer software is run nightly, the reports are reviewed weekly by the IT software procurement manager to validate the licenses. Management signs off on software reports monthly	- Review procedure to ensure illegal software is not installed - Review a 20% sampling of inventory reports - Review current exceptions on file and confirm that they have appropriate supporting documentation.	- Inventory reports - Current exceptions report
		User accounts are locked down at operating system level when they are deployed and enforced with group policy to ensure they cannot install software	- Review the desktop\laptop setup checklist for removal of user admin rights - Review the group policy setting restricting install of software rights - Review current exceptions on file and confirm that they have appropriate supporting documentation.	- Desktop\Laptop setup checklist - Group policy report - Current exceptions report
	Connecting non-standard mobile devices and/or personal computers to the OAS network is prohibited.	Yearly all employees are trained and tested to ensure they understand the acceptable Use policy	- Determine if IT policies are accessible by all employees - Review report showing education on policies exist	- Security Policies
	USB ports on all IT assets must be disabled for the use of portable storage media.	USB ports on all devices are disabled by the IT department before they are deployed for use	- Review laptop, desktop and server setup checklists for the disabling of the USB drive	- Setup checklists
3. Securing and Storing Information To ensure the security, confidentiality, integrity and availability of company information.	OAS computer systems used to store or present any company information to users or third parties must be secured to IT standards	Business owners control access of company information by approving access.	- Review 10% of request tickets for data access to ensure business owner signed off	- Access request tickets
		Members of IT department review forms signed by users acknowledging that company information needs to be encrypted before sharing with the third party.	- Sample of 10% acknowledgment forms obtained from HR	- Acknowledgement forms
	Critical business data must always be managed in such a way that at least one copy is always stored on an OAS server	Any critical business data needs to be authorized by the DBA and backed-up at the mirror site of the OAS data center.	- Review management approval forms and 10% random sample of critical business data	- Current list of critical business data authorized by DBA
4. Labeling and Handling Information Ensure data assets are reviewed and classified depending on the nature of the data. The handling guidelines are	Computer hard drives and other media containing proprietary information, and/or licensed software must be secured.	All computer hard drives are configured to use encryption by the IT department before assets are deployed for use	- Review any approved exceptions and ensure the approved control is in place - Review the asset setup\deployment process to ensure encryption software is installed and enabled	- Current approved exceptions - Current asset deployment processes - Current license for encryption software
		Licensed software and licenses are stored in the configuration management database (CMDB) and access is managed by the IT procurement employee	- Review access controls against 10% of the CMDB software assets	- Current export of CMDB software assets - Current access control list for software asset records

established to ensure data movement is protected depending on the classification	Proprietary information and technical data will not be posted on any computer system accessible to the general public or accessible on the general OAS intranet unless protected by further restrictions.	IT department conducts review of classification of data quarterly	- Review the report conducted by IT department of period under review - Review current exceptions on file and confirm that they have appropriate supporting documentation. - Review policy related to Labeling and Handling information	- Information Labeling and Handling policy - Reports of data classification test by IT department - Current exceptions report
		IT department conducts review of information public on company's public sites monthly	- Review the report conducted by IT department of period under review - Review current exceptions on file and confirm that they have appropriate supporting documentation.	- Reports of data classification test by IT department - Current exceptions report
5. Passwords Control Set of rules designed to enhance system security by encouraging users to employ strong passwords, follow structure of password and keep them protected. Password Controls are implemented by IT manager with support of IT team, overviewed by the IT committee and ratified by the Board.	All System/User level passwords creation must comply with the OAS password policy by following passwords length complexity, aging and lockout.	System administrator configures systems to follow passwords length complexity, aging and lockout time according to password policy.	- Review system configurations for password settings for applications in the audit scope	- Current screen shot of password settings
		IT department verifies Password policy acceptance forms have been signed off during the on-boarding process and yearly training.	-Sample 10% of user's password policy signoffs obtained from the HR department	- Password policy acceptance forms
	All computing devices are secured with the password-protected screensaver with the automatic activation feature set to 10 minutes or less. All users must lock the screen or log off when the device is unattended.	System administrator configures systems to log off the computers within 10 minutes.	- Review system configurations for password settings for applications in the audit scope	- User access request forms, Emails and management approval
		IT department random audits of users locking workstations monthly.	- Review audit checklist "IT security policy checklist" and " Logical security control checklist" is used to support the design, implement and post-implementation review of password controls	- Screenshot of the user's configuration settings
	Password must be protected and login credential should not be revealed to others.	Monthly random physical review of users work area by a member of IT department to ensure passwords are not written down.	- Review report of monthly physical review	- Report of the review
		System administrator configures systems to store passwords in irreversible encrypted form and generate password file in encrypted form.	- Review system configurations for encryption settings for applications in the audit scope	- Current screen shot of encryption settings
	Users must not use another individual's account, or attempt to capture or guess other user's password.	IT department verifies Password policy acceptance forms have been signed off during the on-boarding process and yearly training.	- Sample 10% of user's password policy signoffs obtained from the HR department	- Password policy acceptance forms
		System administrator limits login IDs to the owner of the IT asset.	- Review configurations for login restriction settings for applications in the audit scope	- Current screen shot of login restriction settings

6. Remote connectivity To ensure the overall network security and security requirements for virtual private network (VPN), dial-up, and other forms of connection to external parties	Remote connectivity will be granted based on business need	IT department requires sign off by HR to provide remote connectivity access to OAS systems.	- Review 10% random sample of remote connectivity access requests to ensure HR provided appropriate sign offs	- Request tickets for remote connectivity access
	The users are responsible for keeping the device secure and if the device is lost or stolen, the user is responsible to contact the service desk immediately	Perform user's responsibility training for all OAS users annually and required to sign the acceptance form	- Review 10% random sample of services desk log and acceptance form	- Acceptance forms
7. Client security To ensure security of OAS computer systems."	Security controls (physical locks, removing or installing of security applications) on desktops and/or laptops assigned to them by the company	IT department issues locks and they are distributed to all employees at the issuance of their computer systems which are logged in the asset management system.	- Review 10% random sample of employees and their assigned computer systems to determine if locks were issued	- Current export of CMDB
		Security applications are installed and updated on computer systems by the IT department.	- Review security application logs to ensure they are up-to-date	- Current application logs for security applications
		HR requires employees sign-off on Client Issuance Policy during on-boarding process.	- Review a sample of employee Client Issuance Policy for sign offs	- Current Client Issuance Policy Acceptance forms
8. Social media To ensure OAS' online presence is in line with the brand and accurately represented on internet platforms including, but not limited to, social networking and video platforms, blogs, review sites and forums.	Social media will only be used for authorized business purposes with the approval of the marketing director or authorized manager.	Marketing director or authorized manager will approve essential employees to use social media for business duties.	- Review management approval forms and ensure owner documents social media login information	- Current list of active employees authorized to use social media
	Social media content must be appropriate, accurate and respectful to OAS (including compliance with financial disclosure laws and OAS confidential information).	HR randomly monitors social media profiles at least twice a year	- Review 10% random sample of current employee social media profiles	- Screenshot of social media profiles